CLAIMS

1. A method for providing client access to the Internet or other network, comprising:

5   offering, at a point of service, a Local Area Network (LAN) connected to the Internet or other network;

connecting at least one client computer to said LAN;

configuring networking parameters of each of said at least one client computer;

10   establishing a secure tunnel between the service provider and each of said at least one client computer, such that the service provider provides Internet or other network service through the secure tunnel to only each one of said at least one client computer;

15   negotiating, at the point of service, the network usage terms and prices with each one of said at least one client computer; and

providing the Internet or other network service at the point of service to each one of the at least one client

20 computer in accordance with the network usage terms and prices.

2. The method of claim 1, further comprising establishing a contract at the point of service wherein the contract

25 defines the network usage terms and prices negotiated between the client and the service provider.

3. The method of claim 2 wherein the contract does not depend on a previous or subsequent relationship between

30 client and service provider.

4.   The method of claim 2 wherein the user of the client computer may select as short a contract term as the user of the client computer desires.

5   5.   The method of claim 2 wherein the client's usage is measured by bytes or packets transmitted or received, or by the contract's active or elapsed time.

6.   The method of claim 2 wherein the client may choose a
10   hard usage limit, such that the service provider terminates the contract when the hard limit is reached.

7.   The method of claim 2 wherein the user of the client computer may request contract termination.
15

8.   The method of claim 2 where, after receiving a deposit, the service provider sends to the client computer a receipt that the client computer may use to recover from a client computer or service provider failure, obtaining access
20   again on the same contract.

9.   The method of claim 8 wherein the receipt contains all the information required for recovery.

25   10.   The method of claim 2 wherein the contract is established and the client may monitor and control its usage via a Transport Layer Security protocol or via a Secure Socket Layer connection.

30   11.   The method of claim 1 wherein the service provider owns or rents the premises at the point of access.

12.   The method of claim 1 wherein access is provided in one of an airport, hotel, conference center, or a multi-tenant building.

5   13.   The method of claim 1 wherein a service provider that provides the client access obtains access services from another service provider, e.g., an Internet Service Provider (ISP).

10   14.   The method of claim 1 wherein a service provider that provides client access is connected to the Internet by one or more Digital Subscriber Lines (DSL), T1 or other dedicated telephone lines, Integrated Services Digital Network (ISDN) lines, or cable modems.

15

15.   The method of claim 1 wherein a service provider that provides the client access uses Network Address Translation.

20   16.   The method of claim 1 wherein the network configuration of client computers is automatic.

17.   The method of claim 16 wherein the network configuration of client computers is performed by the
25   Dynamic Host Configuration Protocol.

18.   The method of claim 1 where packets sent from the client computer to or via a service provider are authenticated.

30

19.   The method of claim 1 where packets sent from or via a service provider to the client computer are authenticated.

20.   The method of claim 1 where packets sent between the client computer and a service provider are encrypted.

5   21.   The method of claim 1 wherein the client computer may choose whether packets sent from or via a service provider to the client computer should be authenticated, or whether packets sent between the client computer and a service provider should be encrypted.

10   22.   The method of claim 1 wherein the client may choose how a service provider measures the client's usage.

23.   The method of claim 1 wherein the client may choose a soft usage limit, such that the service provider suspends
15   service to the client when the soft limit is reached and sends a notification to the client, and the client may resume service and set a new soft limit by sending a message to the service provider.

20   24.   The method of claim 1, further comprising the client paying for said Internet or other network service, wherein the payment is offline.

25.   The method of claim 24 wherein payment is by one or
25   more of the following options: cash, credit card, and debiting from another account.

26.   The method of claim 1, further comprising the client paying for said Internet or other network service, wherein
30   the payment is online.

27.   The method of claim 26 wherein payment is by one or more of the following options: eCASH®, SECURE ELECTRONIC TRANSACTIONS (SET)®, IBM MICROPAYMENTS®, or MILLICENT®.

5   28.   The method of claim 26 wherein online payment, no matter how implemented, is performed through an authenticated and/or encrypted tunnel, and therefore is automatically and securely bound to it.

10   29.   The method of claim 1, further comprising paying for said Internet or other network service, wherein a user of the client computer can choose the payment method or a combination of payment methods.

15   30.   The method of claim 1 wherein the user of the client computer may monitor and control the client computer usage.

31.   The method of claim 1 wherein the user of the client computer, before gaining service, pays to the service 20   provider a deposit corresponding to a hard usage limit.

32.   The method of claim 31 wherein the user of the client computer, before gaining service, pays to the service provider a deposit, and, when the user requests contract 25   termination, the service provider returns to the user the difference between the deposit and actual usage.

33.   The method of claim 1 wherein the client computers are not portable.
30

34.   The method of claim 1 wherein the client computers are portable.

35. The method of claim 1 wherein the client computers are wearable.

36. The method of claim 1 wherein the LAN conforms to a
5   standard.

37. The method of claim 36 wherein the LAN is an Ethernet.

38. The method of claim 36 wherein the LAN is an 802.11
10   wireless network.

39. The method of claim 1 wherein security protocols used by the secure tunnel are standard.

15   40. The method of claim 39 wherein the security protocols belong to the IPSec protocol suite of the Internet Engineering Task Force (IETF).

41. The method of claim 40 wherein the client computer
20   uses a self-signed certificate.

42. The method of claim 40 wherein the service provider uses a certificate signed by a Certification Authority (CA).
25

43. The method of claim 42 wherein the Certification Authority (CA) has special procedures for certifying service providers.

30   44. The method of claim 42 wherein the certificate includes the location and type of LAN used by the service provider.

45. The method of claim 42 wherein the packets sent from the client computer to or via the service provider are authenticated using IPsec's Authentication Header (AH).

5   46. The method of claim 42 wherein the packets sent from or via the service provider to the client computer may be authenticated using IPsec's Authentication Header (AH).

47. The method of claim 42 wherein the packets sent
10 between client computer and a service provider may be authenticated and/or encrypted using IPsec's Encapsulating Security Payload (ESP).

48. The method of claim 41 wherein the security protocol
15 is Point-to-Point Tunneling Protocol (PPTP).

49. The method of claim 1 wherein the user of the client computer does not reveal its identity to the service provider.
20

50. The method of claim 1 wherein a secure connection is established between client and service provider, and wherein the secure connection is used to communicate secrets used for establishing a secure tunnel between those
25 parties.

51. The method of claim 1 wherein service provider functionality is implemented by an integrated router/server.
30

52. The method of claim 1 wherein service provider functionality is implemented by separate router and server.

53. A method for providing metered access to the Internet, comprising:

accessing, via a local area network (LAN), the Internet, utilizing a service provider;

5   establishing a secure tunnel with said service provider by exchanging authentication certificates with said service provider;

negotiating network usage terms with said service provider at a point of access to the Internet; and

10   accessing said Internet via said service provider according to said negotiated usage terms.

54.   The method of claim 53, wherein a self-signed authentication certificate is provided to said service 15   provider during said authentication.

55.   The method of claim 53, wherein said usage terms are defined in terms of one of time and bandwidth.

20 56.   The method of claim 53, wherein the contact established between the client and the service provider to access the Internet can last for a duration selected by the client.

25 57.   An apparatus for providing client access to the Internet or other network, the apparatus comprising:

a Local Area Network (LAN) to which client computers can be connected;

a router that connects the LAN to the Internet or 30   other network;

a secure tunnel established between each client computer and the router, such that the router forwards to the Internet or other network only packets sent from the

a server computer with which client computers communicate to negotiate, control, and settle access contracts wherein the server computer controls the router to establish or tear down each client computer's secure

5   tunnel.